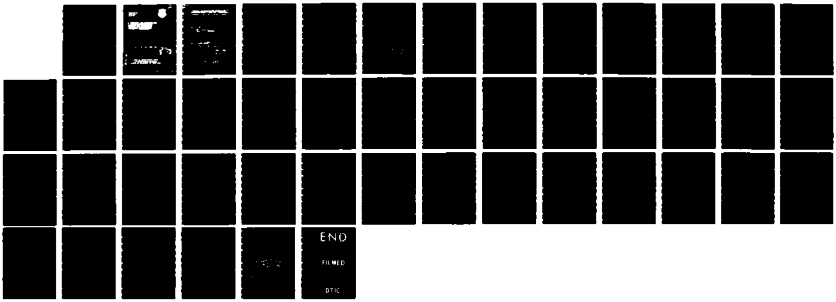
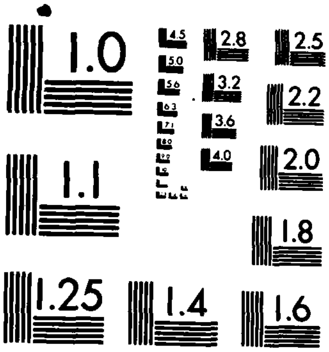
AD-A162 617 A RATIONALE AND APPROACH FOR DEFINING AND STRUCTURING TESTABILITY REQUIREMENTS(U) ROME AIR DEVELOPMENT CENTER GRIFFISS AFB NY J KLION AUG 85 RADC-TR-85-150 1/1

UNCLASSIFIED F/G 9/3 NL




1.0
4.5
2.8
2.5
5.0
3.2
5.6
2.2
6.3
3.6
7.1
8.0
4.0
2.0
1.1
1.8
1.25
1.4
1.6

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

AD-A162 617

REPORT DOCUMENTATION PAGE

1a REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS N/A
2a. SECURITY CLASSIFICATION AUTHORITY N/A	3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution unlimited
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE N/A	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) RADC-TR-85-150	5. MONITORING ORGANIZATION REPORT NUMBER(S) N/A

6a. NAME OF PERFORMING ORGANIZATION Rome Air Development Center	6b. OFFICE SYMBOL (*If applicable*) RBET	7a. NAME OF MONITORING ORGANIZATION N/A
6c. ADDRESS (*City, State, and ZIP Code*) Griffiss AFB NY 13441-5700		7b ADDRESS (*City, State, and ZIP Code*)
8a NAME OF FUNDING/SPONSORING ORGANIZATION Rome Air Development Center	8b. OFFICE SYMBOL (*If applicable*) RBET	9 PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER N/A

8c. ADDRESS (*City, State, and ZIP Code*)
Griffiss AFB NY 13441-5700

10. SOURCE OF FUNDING NUMBERS

PROGRAM ELEMENT NO.	PROJECT NO.	TASK NO.	WORK UNIT ACCESSION NO.
62702F	2338	02	2X

11 TITLE (*Include Security Classification*)
A RATIONALE AND APPROACH FOR DEFINING AND STRUCTURING TESTABILITY REQUIREMENTS

12 PERSONAL AUTHOR(S)
Jerome Klion

13a TYPE OF REPORT In-House	13b. TIME COVERED FROM Jun 83 TO Jan 85	14. DATE OF REPORT (*Year, Month, Day*) August 1985	15 PAGE COUNT 52

16. SUPPLEMENTARY NOTATION
N/A

17 COSATI CODES			18 SUBJECT TERMS (*Continue on reverse if necessary and identify by block number*)
FIELD	GROUP	SUB-GROUP	Testability,
09	03		Diagnostics, and
09	05		Fault Detection/Isolation.

19 ABSTRACT (*Continue on reverse if necessary and identify by block number*)

Testability concepts and requirements are being applied to many Air Force electronic equipment/system development programs. Insufficient guidance exists as to the definition and structure of testability requirements and the interface between such requirements and maintainability, availability, and integrated diagnostics. The purpose of this report is to provide one logical approach and associated guidance to the definition and structure of testability needs and:

1) The relationship of testability to other system parameters,
2) The translation of testability needs to testability requirements,
3) The interpretation of testability terms, concepts and requirements,
4) The structure and scope of testability requirements, and
5) The identification of those factors, constraints and contingencies which must be considered when invoking testability requirements. [illegible]

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT □ UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT □ DTIC USERS	21 ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED

22a NAME OF RESPONSIBLE INDIVIDUAL Jerome Klion	22b TELEPHONE (*Include Area Code*) (315) 330-4726	22c OFFICE SYMBOL RADC (RBET)

83 APR edition may be used until exhausted.
All other editions are obsolete.

SECURITY CLASSIFICATION OF THIS PAGE

UNCLASSIFIED

TABLE OF CONTENTS

FIGURES

PREFACE

Testability both as a concept and as a requirement is being applied to most new Air Force electronic equipment/system programs. In many instances testability considerations and requirements applied have been subject to ambiguous definition and use. In all instances insufficient guidance exists as to the definition and structure of testability requirements and the interface between such requirements and maintainability, availability, and integrated diagnostics. The purpose of this report is to provide information and rationale pertaining to one logical approach to the definition and structure of testability needs and:

1) The relationship of testability to other system parameters.
2) The translation of testability needs to testability requirements.
3) The interpretation of testability terms, concepts and requirements.
4) The structure and scope of testability requirements.
5) The identification of those factors, constraints and contingencies which must be considered when invoking testability requirements.

1. Testability - Its Impact

Testability is a system/equipment attribute which addresses the capability to accurately detect and isolate failures. It impacts both the time and the maintenance manhours/effort required to perform fault detection, localization and isolation activities. These three activities usually consume more time and resources than all the other corrective maintenance actions, associated with a failure, combined. Performance monitoring, another facet of testability, has a direct impact on mission success and on maintenance actions. False alarms, another impact of testability design, can be a major problem in itself. Frequent false alarms contribute to Can Not Duplicate (CND) and RTOK (Retest OK) rates and cause additional unnecessary maintenance actions. Because of these impacts, the testability characteristics of a system/equipment drive its maintainability characteristics and manpower needs, and significantly affect operational readiness.

1.1 Testability - Its Relationship to Maintainability

System Mean Time to Repair, describes the average corrective maintenance time expended for all system/equipment faults. MTTR is the elapsed time from start of work on a malfunction indication to the completion of the maintenance event and verification of the correction. It is the most commonly used maintainability parameter.

$$\text{MTTR} = \frac{\sum_{i=1}^{N} \lambda_i \quad M_{CT_i}}{\sum_{i=1}^{N} \lambda_i}$$

where N = number of system hardware components

λ_i = failure rate of the i^{th} hardware component

M_{CT_i} = inherent mean repair time for the i^{th} hardware component.

M_{CT_i} is a function of Fraction of Faults Detected, Fraction of Faults Isolated, Mean Fault Detection Time, Fault Isolation Ambiguity, and Mean Fault Isolation Time, as well as set-up time, remove/repair/replacement time, checkout time. One simple model for M_{CT_i} may be represented as follows:

(Assuming fault isolation to a single unit)

$$M_{CT_i} = (FFD_1)(T_{FD1})+(FFD_2)(T_{FD2})+(FFI_1)(T_{FI1})+(FFI_2)(T_{FI2})+T_{SU}+T_{RR}+T_{CU}$$

More complex models can be constructed which take into account different Ambiguity Levels of Isolation, Fraction of False Status or Isolation Indications, and Fraction of False Pulls.

where

FFD_1 = fraction of faults detected by a particular set of means

FFD_2 = fraction of faults not detectable by that particular set of means

T_{FD1} = mean fault detection/recognition time of faults belonging to FFD_1

T_{FD2} = mean fault detection/recognition time of faults belonging to FFD_2

FFI_1 = fraction of faults isolated by a particular set of means

FFI_2 = fraction of faults not isolated by that particular set of means

T_{FI1} = mean fault isolation time of faults belonging to FFI_1

T_{FI2} = mean fault isolation time of faults belonging to FFI_2

T_{SU} = mean setup time

T_{RR} = mean remove/replace/repair time

T_C = mean checkout time

MTTR is one of the measures of system design adequacy for meeting operational needs and is a major component of operational readiness or availability.

1.2 Testability - Its Relationship to Availability

System Availability is a measure of the degree to which the system/equipment is in an operable and committable state at the start of a mission, when the mission is called for at an unknown (random) point in time. Inherent availability is often defined as:

$$A = \frac{MTBF}{MTBF + MTTR}$$

In order to get an appreciation of the impact of testability attributes on inherent availability, reference is made to 1.1 where MTTR is broken down into its testability parameters.

2. Testability - Its place in Systems Engineering and in the Acquisition Process

Due to the direct impact of testability on maintainability it is both logical and expedient to include testability requirements and needs under the maintainability program plan. Steps have been taken to revise MIL-STD-470 (MIL-STD-470A - Maintainability Program for Systems and Equipment) and MIL-STD-471A (Interim Notice 2 USAF, Maintainability Demonstration) such that testability characteristics, analyses, evaluation, trades and demonstrations may be specifically addressed. These will be discussed later. The consideration/treatment of testability should be initiated as early as possible in the acquisition phase. In some instances, consideration may be appropriate as early as the conceptual phase. In the majority of instances consideration and treatment should start during validation and continue logically through the full scale engineering development phase. Guides as to which testability tasks are appropriate to the various acquisition phases can be found in Appendix A to MIL-STD-2165 (Testability Program for Electronic Systems and Equipments).

3. Testability - Its Makeup

Every system is comprised of removeable units. Once a system failure is detected and localized to a particular equipment, the failed unit(s) in that equipment must be isolated. Test systems, performance monitoring and diagnostics in general can be used to effect such actions. Means through which systems diagnostics and test can be addressed may include:

a. Integrated (designed in portions of the system/equipment) built-in-test (BIT), which operates automatically or on demand;

b. External test equipment used by a maintenance technician. The external test equipment can be either a special purpose piece of equipment or, in the case of intermediate level maintenance, a programmable tester;

c. Manual test and diagnostic procedures requiring the use of technical manuals, troubleshooting procedures, general purpose test equipment, and maintenance technicians;

d. Operator and maintenance technician observations and various forms of performance monitoring;

e. A combination of the above.

The choice of which is most appropriate is dependent upon a variety of factors including the prime system/equipment needs, characteristics, complexity and the cost/benefit ratio for each alternative. The process through which the most efficient and cost effective mix of diagnostics means is determined is known as Integrated Diagnostics. Integrated Diagnostics may be defined as a structured process which maximizes the efficiency of operational & maintenance diagnostics by integrating pertinent elements such as test methodology, automatic and manual test equipment, training and maintenance aids, to provide an overall cost effective capability to detect and unambiguously isolate all faults known or expected to occur in weapon systems and equipment taking into account the mission requirements. Except for the most simple, uncomplex systems, some combination of test system types and diagnostics will be most appropriate. Testability makes up the infrastructure of Integrated Diagnostics.

For the design of testable systems, the following factors should be kept in mind:

a. BIT requires design and integration of additional internal prime system/equipment hardware and software, and the cost of design and acquisition of these elements are as costly as the design of equally complex portions of the prime system/equipment itself. For complex systems or systems made up of many units the cost required to realize automatic isolation to a unique (single) failed unit(s), generally becomes excessive if it is required for a very large proportion of all failures (say significantly greater than 90%).

b. External testers in general also incur design and production costs (even if an existing tester is used, programming costs must be incurred) and can require test points, junctions (and sometimes additional circuitry added to the prime system/equipment) to be designed into the prime system/equipment. In addition, technical manuals must be prepared for the technician relative to the use and maintenance of the tester and perhaps even training may be required. In general, resultant localization and isolation time is significantly greater than would be expected if BIT were employed.

c. Manual test and diagnostic procedures require the acquisition of detailed technical manuals, the development of comprehensive trouble shooting procedures, and, sometimes, the acquisition of general purpose or specialized test equipment. Manual test and diagnostic procedures also require technicians with higher skill levels and a greater level of technical training in prime equipment/system maintenance. In addition, more test points would have to be incorporated into the prime system/equipment design. In general, resultant isolation time is significantly greater than would be expected if external testers were employed.

d. A formal testability design/analysis task(s) is required to adequately assess the effectiveness and cost of each diagnostic alternative.

4. Testability - Its Application to Different Maintenance Levels

Testability must be treated as a separate entity for each level of maintenance, (organizational, intermediate and depot):

a. Testability at the organizational level pertains to fault detection, localization, isolation, false alarms/could not duplicates at the prime system/equipment level, relating to the status of one or more removable units and to the quantity of removals (false removals) sent to shop which are fault free.

b. Testability at the intermediate maintenance level pertains to fault verification and isolation of the units removed from the prime system/equipment, to one or more shop replaceable units. This aspect of isolation is also subject to false indications of failure, false removals, etc.

c. Testability at the depot maintenance level pertains to fault verification and isolation of the subunits removed at the intermediate maintenance level.

5. Testability - Parameters, Definitions and Terminology

In order to structure requirements, the building blocks which make up the requirement must be unambiguously defined. One of the largest problems encountered in early attempts to specify and demonstrate testability has been ambiguity and confusion in the definition and application of parameters. For example, one testability figure of merit in common use as a testability requirement is Fraction of Faults Detected (FFD). It has been defined quantitatively in the past as this:

$$\text{FFD} = \frac{\text{Quantity of actual failures detected}}{\text{Quantity of failure indications}}$$

with no further information provided.

The term failure indications in this case is ambiguous. A failure causes a failure indication, to be sure, but so does a false alarm. Secondly, the definition provides no direction as to whether or not to take failure rate into account in designing toward this parameter. (There is a difference between saying 90% of all possible failures should be detected and saying 90% of all failures expected to occur during operational life should be detected). Thirdly, no indication has been given as to who is to do the detecting, the operator during system operation, or the maintenance technician during checkout or inspection, or both operator and technician. In the sections which follow, an attempt has been made to structure and define (redefine) such parameters as unambiguously as possible.

5.1 Ambiguity Level or Resolution

Ideally, given just the information that a failure has occurred in a given system/equipment, or unit, immediate isolation to a single removeable unit or subunit would be desirable. Realistically, however, due to cost and/or engineering constraints, situations occur where such unique identification is not practical. Consequently, isolation may initially take place to a group of X removeable units (subunits), only one of which may be faulty. In this case, X is defined as the Fault Ambiguity Level or Fault Resolution Level for a given test means. Additional procedures would then be required to isolate the failure to a specific faulty unit.

WHAT YOU SHOULD KNOW ABOUT AMBIGUITY

When an ambiguity level exists, consideration must be given to the means through which eventual isolation to the faulty unit(s) can be affected. Several alternatives are possible:

a. Isolation to the faulty unit (subunit) at the organizational (intermediate) maintenance level through the use of semiautomatic or manual test means after the group containing the failed item has been identified.

b. Repetitive remove/replace/checkout actions on the units (subunits) making up the group at the organizational (intermediate) maintenance level until the faulty item is isolated.

c. Under critical mission pressures, removal and replacement of all members making up the group, with isolation to the faulty members taking plare at the next maintenance level.

All of the above alternatives impact maintenance manhours, mean time to repair (via isolation and remove/replace/checkout actions) and acquisition cost (via hardware/software cost incurred in order to effect isolation from a given group) in different ways. The various impacts on time and resources must be considered when defining the maintenance actions required to handle ambiguity levels. The magnitude of the ambiguity level itself also has obvious impacts on the maintenance manhours, mean time to repair required and logistics costs as well. The contractor should be required to consider such alternatives, and make recommendations as to the most cost/mission effective means to be employed (Provided the Government does not specifically specify a given procedure to be followed).

5.2 Fraction of Faults Detected (FFD)

Failure detection in general may be viewed as the determination and display of an item (system, equipment, unit) malfunction either directly or indirectly, to its operator or to other appropriate personnel (maintenance technician, observer, etc.) through the use of defined procedures and processes.

Faults in general should be directly detectable by an operator (determination and display of malfunction) through various means:

a. Inspection - The operator is the test system (if a radio receiver fails to receive, no hardware/software test system is required to impart evidence of failure to the operator).

b. Automatic means on or off line, including BIT and performance monitoring.

c. Semiautomatic Means (BIT or specified system trials) by interrogation on-off line.

Faults also may be indirectly detectable to an operator through remote means (communication is received from a remote area that a particular transmission is garbled or absent).

In addition, faults may also be directly detectable to a maintenance technician through:

a. Semiautomatic means (during specified performance checks or a specified series of system trials) by interrogation, on or off line.

b. Manual means, including manual system and equipment checkout procedures periodically performed by maintenance technicians (e.g., Pre- and Post- mission checks).

Not all failure detection schemes or test systems based soley on direct inspection and/or automatic display of failures to the operator will be capable of detecting all possible faults (under practical funding and engineering constraints). Examples include phased array radar systems, missiles, and fault tolerant systems. Even when the additional option of semiautomatic means of failure detection is available for operator exercise the attainment of 100% direct operator fault detection capability may be impractical. Recognizing this, and since its has become common practice to associate failure detection primarily as an operator function tied to strictly automatic, or a combination of automatic and other direct means, the specification for fault detection is commonly expressed in terms of Fraction of Faults Detected (FFD). In certain instances however, failure detection by a maintenance technician (as well as by an operator) under a prescribed set of circumstances may be satisfactory as may be failure detection through indirect means. In those instances the term Fraction of Faults Detected (FFD) is still employed but definition of who will perform the detection and under what conditions detection will take place must be made.

In defining FFD as a contractual requirement for most programs, it is sometimes simpler to exclude those types of direct detection means (for example detection through the use of technicians) which would in general be unsatisfactory to a given mission environment than to define those that are acceptable. The fact that an FFD requirement is imposed should not imply that 100% of all expected failures should not be detectable. The contractor should be tasked with the development of cost effective, defined procedures to detect all expected failures. All of these however, need not be direct means or belong to the type of direct means which are defined as satisfactory for general mission operational use, provided maintainability and other requirements can still be met. As indicated previously, detection can include direct or indirect indications to an operator, the use of maintenance technicians or other personnel performing in accord with a series of defined routines, or some combination of these. When the time required to make a detection is mission critical a Mean and/or Maximum Failure Detection Time requirement should be imposed as well.

WHAT YOU SHOULD KNOW ABOUT FFD

* FFD can be defined as that fraction of failures which occur over operating time which can be correctly identified through direct observation or other specified means by an operator and/or other specified personnel under a given set of conditions. Reference is made to Appendix A for a quantitative definition of FFD.

* In specifying (FFD), all the various means which can be used to detect faults must be taken into consideration. (See Appendix B for General Guidelines for specifying those means appropriate to perform detection based on the mission criticality of the end item). The requirement for FFD should be stringent enough to exclude the application of the types of detection means which are unsatisfactory/unacceptable for the system needs/objectives/philosophies, but flexible enough to allow the contractor to cost effectively tailor his design. In general, the specific nature and mix of the means to be employed to achieve a given minimum (FFD) should be dependent upon results of an analysis of each such alternative and its cost and performance effectiveness in conjunction with other system/equipment design factors and requirements. The contractor should be tasked to perform such analyses and provide results/recommendations based on these to the procuring activity.

* The FFD specification parameter must be specifically defined to take into account frequency of failure (failure rates) of the components making up the system. It is only in this way that FFD will be representative of what occurs during operational life.

* In specifying FFD, care must be taken to define that set of detection conditions which are acceptable, for example, who can perform the detection function; what are the acceptable means through which detection can be performed; during which equipment status modes may detection be performed (operation, pre or post mission checks etc.); whether or not a failure must be detected within a period of time.

* Generally speaking in order to design for fault detection, techniques such as a failure modes and effects analyses (FMEA) are required. If such a task is necessary, that analysis should be integrated into and coordinated with other similar analyses which must be performed for other purposes.

* In order to verify that a FFD requirement has been achieved a demonstration must be called out as a requirement. MIL-STD-471A, Notice 2 (Maintainability Verification/Demonstration/Evaluation) contains test plans for this purpose.

* Since a given fault detection scheme or test system may not be capable of detecting all known or expected faults, provision must be made to develop back-up or ancillary fault detection means (indirect means, periodic performance monitoring, pre or post mission checks etc.) such that 100% of expected faults are detectable through *some set of defined* means.

5.2.1 Fraction of Critical Faults Detected (FCFD)

FFD is general in nature and can be applied at either a system or system component level. Fraction of Critical Faults Detected (FCFD) is a special case of FFD which is usually applied only at a system level. FFD includes all item failures both critical and non-critical. FCFD includes only those faults which are critical. A critical failure may be defined as a failure in a system which places the system in an operational state such that the mission is jeopardized or that a hazard to either personnel or resources exists. Take for example, a system comprised of three computers.

The system can perform its function satisfactorily with only mild degradation with two units operating but failure of two or more without that knowledge being apparent to the operator would seriously jeopardize the success of the mission. While it is important that all computer failures be detectable by the operator, it is critical that the operator be aware of the fact that two or more computers have failed. Hence an FCFD = .999 might be required of the system where FFD requirements on each unit could be less stingent.

5.3 Fraction of Faults Isolated (FFI)

Fault Isolation in general may be viewed as the isolation of a failure down to a particular removable unit (subunit, subunit component), or a defined group of removable units (fault ambiguity level) by a maintenance technician through the use of defined diagnostic procedures and processes. Failures may be isolated through various means:

a. Automatic means (BIT or external testers) on or offline, down to the defined ambiguity level or faulty item.

b. Semiautomatic means (BIT or external testers) on or offline down to the ambiguity level or faulty items.

c. A prescribed series of manual tests and observations.

d. Signal tracing and analyses through the use of schematics and test equipment.

e. Repetitive item remove, replace and performance check actions.

f. Hot-mockups •

g. Any combination of the above.

While literally any fault can be isolated uniquely given an unlimited amount of time and resources, no single fault isolation procedure or diagnostic means (system) may be capable of isolating all possible faults (under practical or reasonable funding, manpower, mission time and engineering constraints). That fact holds for isolations performed at all three levels of maintenance. Furthermore every system, mission scenario and maintenance echelon has its own specific characteristics, constraints and needs which may make one particular diagnostic or isolation means (or a specific combination of means) acceptable and others, in general, not acceptable (although they may be acceptable in an exceptional circumstance, when other means fail, or as a fallback position). As a consequence, requirements relative to isolation of faults should be coached in terms of Fraction of Faults Isolated through the use of one, or a combination of, defined acceptable diagnostic means (which would be satisfactory for general use in that mission/maintenance environment). For example one could specify that 90% of all faults which occur in operation must be isolatable through the use of automatic diagnostic means. (See Appendix A for quantitative definition.)
An alternative to the above would be to define the Fraction of Faults Isolated requirement and to exclude those diagnostic/test means which are unacceptable to a given mission or use environment. For example one could specify that 90% of all faults which occur in operation must be isolatable without the use of test points, probes, or general purpose test equipment.

While any number of means of isolation may be acceptable, some may be so time consuming that readiness would be severely impacted. For this reason it is critical to either integrate the FFI requirement with a maintainability requirement (Mean Time to Repair, Maximum Percentile of Maintenance Time Allowed) or to impose a Mean and/or Maximum Time requirement on isolation time.

Faults may be isolated down to a specific removable unit (subunit, subunit component) or to a group of such items (see 5.1 for a discussion of ambiguity.) If system needs dictate that isolation be performed to the failed unit(s) (ambiguity level 1) without regard to how this is to be accomplished an example of the requirement imposed might read "90% or more of all faults occurring in operation must be isolated to the failed unit using any combination of defined acceptable automatic, semiautomatic or manual means". If system needs dictate that isolation can/should be accomplished just to a given maximum level of ambiguity and that there exists a specific set of means which should be employed for this purpose, an example of the requirement imposed might read "90% or more of all faults occurring in operation must be isolated to a maximum ambiguity level of three units through the use of automatic means". If system needs dictate that isolation be performed to the failed unit(s) and further that the use of specific diagnostic means be maximized, an example of the requirement imposed might read "90% of all faults occurring in operation must be isolated to a maximum ambiguity of three units using automatic means. Additional semiautomatic or defined manual means will be developed if necessary to provide isolation from the ambiguity group, to the faulty unit(s)". In all instances, when an ambiguity level is cited consideration should be given as to where, how, and through which means isolation to the faulty unit(s) will (or can) take place. Consideration must be given to certain questions. How can that second tier fault isolation be implemented at the organizational or the intermediate level of maintenance? Which means are acceptable (desirable) to perform that function?

A requirement of this nature should not provide the impression that (1-FFI) of all expected faults do not have to be isolatable. 100% of all expected faults must be isolatable but a certain fraction (1-FFI) may have ambiguity levels greater than the value stated or be isolatable through means which are definable but which do not belong to the class of diagnostic means cited as being acceptable for general use in the given mission or use environment. Again consideration must be given as to how and where isolation to the faulty unit(s) must take place.

WHAT YOU SHOULD KNOW ABOUT FFI

* FFI can be defined as that fraction of failures which occur over operating time that can be correctly isolated to x units or fewer at a *given maintenance echelon through* use of specified means, by a maintenance technician or other specified personnel. Reference is made to Appendix A for a quantitative definition for FFI.

* In specifying FFI, all the various generic means acceptable in general for the mission/operational/maintenance environment which can be used to isolate faults must be taken into consideration. The requirement for FFI should be stringent enough to exclude the application of isolation means which are known in general to be unsatisfactory/unacceptable to the system needs/maintenance philosophy/objectives but flexible enough to allow the contractor to cost effectively tailor his design. The specific nature and

mix of the means to be employed should be dependent upon the results of an analysis task (levied on and performed by the contractor) of each fault isolation alternative in conjunction with system/equipment design factors, maintainability requirements and support system needs. Generally speaking unless there is clear evidence that unacceptable weight volume, or cost penalties would accrue otherwise, primary diagnostic means based on, (1) signal tracing and analyses through the use of schematics and test equipment and (2) repetitive item remove/replacement/performance check actions should be avoided.

* In specifying FFI care must be taken to indicate the conditions under which isolation must take place:

a. Where it takes place (i.e., organizational level, shop level).

b. What are the acceptable means of isolation (i.e., built in test, external testers, general purpose testers, peculiar testers, manual means, degree of manual means.)

c. Who will perform the isolation (i.e., operator or maintenance technician.)

d. Its constraints (i.e., prohibition of wholesale removal of units, time allowable.)

e. Its second isolation tier requirements (what happens after isolation to proper ambiguity level).

f. The time constraints levied by the maintainability requirement.

* The FFI parameter must be specifically defined to take into account frequency of failure (failure rates) of the components making up the system. It is only in this way that FFI will be representative of what occurs during operational life.

* Generally speaking in order to design to a required FFI, a failure modes and effects analysis (FMEA) must be performed. If such a task is necessary that FMEA should be integrated and coordinated with FMEA's performed for other purposes.

* One given diagnostic means or even a given combination of acceptable means may not be capable of completely isolating 100% of all the faults known or expected to occur within given constraints. Provisions must therefore be made, if necessary to develop additional suboptimum (but defined) fault isolation means or procedures which are capable of isolating the remainder of all faults which can occur. Engineering, maintenance and cost constraints must be considered when specifying and developing such isolation schemes and/or procedures.

* In order to verify that a FFI requirement has been achieved a demonstration must be called out as a requirement. MIL-STD-471A, Notice 2 (Maintainability Verification/Demonstration/Evaluation) contains test plans for this purpose.

* FFI and ambiguity level can be traded off. Generally speaking FFI increases as ambiguity level increases.

* Once a design has been transitioned into an operational system/equipment, it may experience unforeseen failure effects. For dealing with unforeseen failure effects, consideration should be given to:

a. Contractually permitting the failure effects "set" to continuously grow (and for isolation scheme or diagnostic test system modifications) through system testing and deployment

or

b. Requiring that a general backup means of troubleshooting, with necessary test points, schematics, technical manuals and test equipment be developed/provided, such that manual test and isolation may be effected.

Feasibility, practicality and cost should be considered carefully on an individual system/equipment basis prior to invoking either of the above.

5.4 False Alarm Rate Ratio

A false alarm is defined as an apparent indication of failure when in fact no failure exists. False alarms are caused by many factors: errors in test system design; transients introduced into, or by the prime system/equipments; or unforeseen changes in the design characteristics of the prime system/equipment or other causes. The false alarm rate ratio is defined as the ratio of false alarm rate to prime system/equipment single thread failure rate (assumes all system/equipment units are connected in series). This represents the ratio of false alarms to failures over any period of operating time or test. For example, a false alarm rate ratio of 1 would denote that the number of false alarms experienced are equal to the number of prime system/equipment failures experienced and hence would connote a moderate to high degree of uncertainty with respect to system/equipment failure indications. This factor of uncertainty is often inadvertently overlooked when false alarm rate is treated as a separate entity and specified as such. (See Appendix A for quantitative definition.)

WHAT YOU SHOULD KNOW ABOUT FALSE ALARM RATES

* Intermittent faults can be difficult to distinguish from false alarms during operational test and in use. A properly structured qualification test, however, can exclude the influence of intermittent faults. Intermittent faults should be controlled under the reliability program.

* False alarm rates are controllable through the use of such design techniques and features as:

a. Scope and magnitude of performance monitoring.
b. Definition of test tolerances.
c. Transient monitoring and control.
d. Multiple run decision logic.
e. Environmental effects filtering and identification.

All have impact on system/equipment design and cost. In general, the decision as to which design procedures and considerations should be adopted to minimize and/or control false alarm rate should reside with the contractor. The contractor, however, should be required to submit a program toward this end for Program Office approval, indicating which steps will be taken to control false alarms and to establish a suitable program for their suppression and control.

5.5 Fraction of Erroneous Fault Isolation Results (FEFI) - The fraction of BIT, or external tester isolations that identify the wrong removable unit (subunit) or group of units (subunits) as failed. FEFI is primarily a design problem resulting either from test system design error, or low sensitivity thresholds and tolerance levels of system/equipment components and/or signals. It can have serious consequences by creating confusion during fault isolation and by eroding maintenance technician confidence in the test system. (See Appendix A for quantitative definition.)

WHAT YOU SHOULD KNOW ABOUT FEFI

* Erroneous Fault Isolation Results may be minimized or eliminated through the use of adequate design control, surveillance, and test.

* Verification tests can be structured to demonstrate FEFI compliance.

5.6 Other Testability Measures and Terms

The following represents secondary or special case testability parameters.

5.6.1 Mean and/or Maximum Fault (Failure) Detection Time - The average and/or maximum time to detect a fault once it has occurred. (Maximum time should usually be defined in terms of a 90th or 95th percentile)

5.6.2 Mean and/or Maximum Fault (Failure) Isolation Time - The average and/or maximum time required to isolate a fault once it has been detected. (Maximum time should usually be defined in terms of a 90th or 95th percentile)

5.6.3 Fraction of Faults Detectable by BIT - Special case of FFD parameter discussed in 5.2.

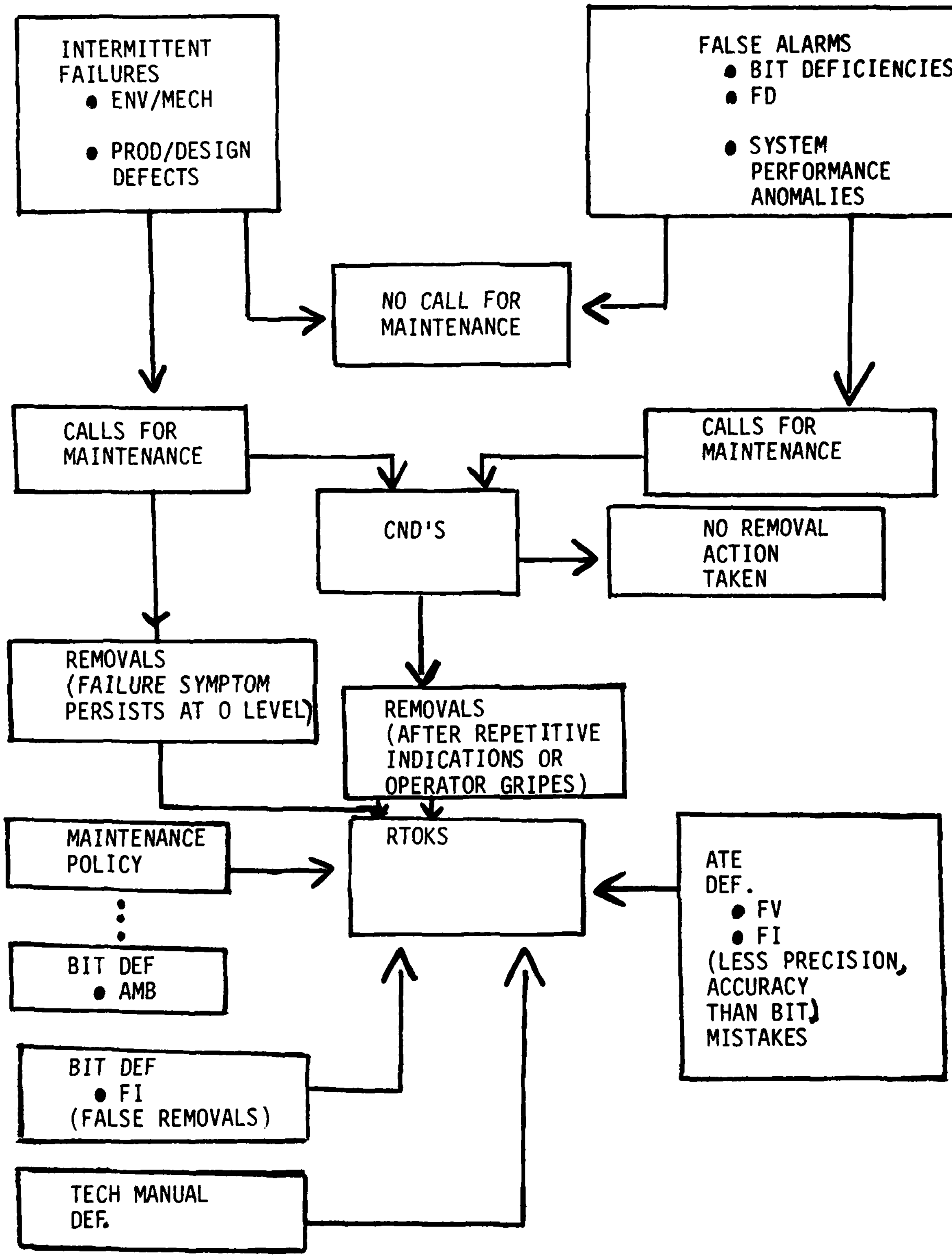
5.6.4 Fraction of False Pulls - The fraction of removable units removed from a system/equipment, due to the result of the fault isolation process, that are not faulty.

5.6.5 Can Not Duplicate (CND) - After a BIT indication of a fault, the finding of no fault indications upon subsequent verification tests or trouble-shooting at the organizational maintenance level. A CND can be caused by factors such as improper test tolerances, momentary excursions, intermittent faults, false alarms, or the inability to produce the same environmental conditions that existed when the failure was originally indicated.

5.6.6 Retest OK (RTOK) - A RTOK occurs when a malfunction which, when detected and isolated at one level of maintenance, is not verified at the next higher maintenance level. A RTOK can be caused by factors such as false alarms, intermittent faults or improperly assigned test tolerances.

FIGURE I

Relationship between False Alarms and CNDs and RTOKs



5.7 The relationship between False Alarms and Can Not Duplicates (CND) and Retest OKs (RTOK) - There is a relationship between false alarms and can not duplicates (CND) and Retest OK (RTOK) rates but the relationship is neither direct nor exclusive. As shown in an example operational scenario, Figure 1, false alarms caused by either Built-In-Test fault detection (FD) deficiencies, system performance anomalies or other factors can result in CNDS, however, in many instances the operator may be convinced that the apparent indication of failure is a false alarm and not even report it. Intermittent failures in the system caused by unforeseen changes in system performance characteristics due to the operational environment, which effect either electronic or mechanical components; installation errors and indirect causes such as wiring; production and design defects in the system, and other factors can result in CNDS. In many instances, however, such failures do not necessarily always result in a CND; the problem may be of such short duration that it may not even be reported or the failure manifestations may be of sufficiently long duration (or at the time repeatable) such that the maintenance technician classifies it as a failure and removes it.

RTOKS are made up in general of those portions of the population of intermittent failures and false alarms which resulted in removals; those units removed due to deficiency in BIT failure isolation (FI) (indicated the wrong unit was in a failed state); Technical Manual deficiencies; Maintenance policy, with respect to organizational level unit removal in general, and in particular in combination with BIT deficiencies with respect to Ambiguity; Automatic Test Equipment (ATE) deficiencies with respect to Failure Verification (FV) and Isolation (ATE less precise than

BIT, ATE errors etc) and others. As can be seen, false alarms contribute to CNDS and RTOKS but so do other factors, some of which are controllable through testability design parameters (for example BIT and ATE, Ambiguity, Fault Detection, Fault Isolation, Fault Verification Parameters). However, some causes of CNDs and RTOKS aren't controllable through testability design (for example Technical Manual deficiencies, Maintenance Policy and Intermittent Failures).

6. Testability - Structuring Requirements - Using the content of the preceeding sections and by applying the quantitative definitions of terms in Appendix A it is possible to structure statement of work (SOW) inputs for testability.

The following provides guidance and examples of the specific types of SOW inputs necessary for tailoring organizational level testability requirements. This example can be logically extended to other levels of maintenance.

6.1 Minimum General Requirements for the Treatment of Testability Specifications

(a) Testability characteristics and parameters are related to, and shall be treated as, part of the maintainability program. Testability parameters shall be treated as additional maintainability terms.

(b) Progress relative to the attainment of testability requirements shall be reported as part of maintainability program reviews.

(c) Testability analyses, design characteristics and tradeoff efforts and results will be integrated into and utilized to form a foundation for maintainability modelling, prediction, analyses and design.

(d) Factory demonstration of each testability requirement shall take place as part of the Maintainability Demonstration in accordance with MIL-STD-471A, Interim Notice 2, (USAF) procedures or other means as defined.

(e) Testability requirements must be consistent with the Integrated Diagnostics policy which requires that all faults known or expected to occur in a system/equipment be detectable and isolatable through some defined means. (Note that in accord with the rationale developed FFD and FFI *specifications require that fraction of faults be detected and* isolated through the use of defined means which are acceptable or appropriate for general usage in the given mission/operational/maintenance environment, under a given set of conditions or constraints.)

6.2 Specification of FFD Requirements

The following make up an example specification requirement outline for FFD:

(a) The system/equipment shall have a minimum Fraction of Faults Detected (FFD) = P_1 (define FFD as in Appendix A) during normal operator operation. (If appropriate, indicate any time constraint on detection)

(b) FFD shall be defined taking into account the relative failure rates of the components making up each end item.

(c) Design and engineering studies shall be undertaken to determine the specific nature and mix of the means to be employed in detecting faults. Such design studies shall take into account not only the various means available to achieve the FFD requirements but also cost and the impact on other system/equipment requirements.

(d) Predictions of FFD for each level of system/equipment indenture shall be made, based on engineering analyses and Failure Modes and Effects Analysis (FMEA) data generated.

(e) Design engineering provision shall be made to provide system/equipment diagnostic procedures capable of detecting 100% of system/equipment failures either directly or indirectly by its operator or through the services of maintenance technicians or other personnel performing under a series of defined routines (without the need for system/equipment disassembly).

6.3 Specification of FFI Requirements

The following make up an example specification requirement outline for FFI:

(a) The system/equipment shall have a minimum FFI = P_2 with maximum ambiguity level X_1 (define FFI as in Appendix A providing the necessary constraints and conditions required as discussed in "what you should know about FFI", pages 17-19).

(b) FFI shall be defined taking into account the relative failure rates of the components making up each end item.

(c) The FFI requirement shall be integrated/coordinated with the maintainability requirement.

(d) Design and engineering studies shall be performed to determine the specific nature and mix of the means (automatic, semiautomatic, manual), to be employed to achieve the fault isolation requirements. Such design studies shall take into account not only the various means available to achieve the FFI requirement, but their cost and impact on other system/equipment requirements as well (i.e., maintainability, weight, etc.).

(e) Such studies will form the basis for: (a) determining the various ambiguity levels associated with each individual isolation, (b) the remove/replace, diagnostic or maintenance policy to be applied to each given level of ambiguity (isolation to faulty unit given primary isolation is made to a group of units, only one of which may be fault) unless that policy is provided to the contractor by the Government.

(f) Predictions of FFI for each level of system/equipment indenture shall be made, based on engineering analyses and Failure Modes and Effects Analysis (FMEA) data generated.

(g) The fraction of faults isolatable to an ambiguity level higher than X_1 shall be defined and documented.

6.4 Specification of False Alarm Requirements

A high false alarm rate can represent a very real operational problem. Measures should be taken durinq the design of a system/equipment to assure that false alarm rates are controlled. The following inputs have been developed for use in the design phase to support the control of false alarms:

(a) The system/equipment shall have a maximum false alarm rate ratio = P_3 where false alarm rate ratio is defined as the ratio of false alarm rate to system/equipment single thread failure rate (single thread failure rate is the failure rate that would result if it were assumed that the failure of any component making up the system/equipment would cause system/equipment failure) (define false alarm ratio as in Appendix A).

(b) False alarm suppression engineering studies shall be performed based on system/equipment needs to identify design criteria and determine the means through which false alarm rate may be controlled and minimized.

(c) To the extent possible false alarm rate will be verified using data from reliability and other tests.

(d) Operational test results and findings shall serve as an additional basis to correct false alarm deficiencies not apparent during factory tests.

7. Testability - Program Structure and Maintainability Interface.

7.1 Program Tasks - Whenever testability requirements are levied, a series of program tasks related to those requirements must be addressed by the contractor and properly integrated with other program elements. The following identifies such tasks and provides guidelines for their integration into the maintainability program:

7.1.1 The Testability Program Plan - Outlines the planning, and identifies and integrates all testability related tasks to be performed - Provisions for such a plan should be either referenced in the Maintainability Program Plan and expanded in an Ad Hoc Testability Program Plan or directly integrated into the Maintainability Program Plan.

7.1.2 Testability Reviews - Provides the Government means to review testability design information in a timely and controlled manner. Such reviews should be integrated into maintainability reviews.

7.1.3 Testability Data Collection and Analysis Plan - Establishes methods for identifying and tracking testability related problems during systems production and deployment and identifying corrective actions - Provision for such a plan should be integrated with or into the Data Collection, Analysis, and Corrective Action System (DCACS) of the maintainability program. In the case when an Ad Hoc Testability program is invoked it should be referenced in the DCACS and provision made to integrate and coordinate its requirements and needs with DCACS elements. When an Ad Hoc Testability program is not invoked the plan should be directly integrated as a part of the DCACS.

7.1.4 Testability Allocation and Planning - Establishes testability design objectives, and allocation of testability requirements to lower levels of system indenture, and defines on and off line test objectives. Results of such a task should be integrated with (or done under the auspices of) the Maintainability Allocation Task, the Maintainability Prediction Task and the Maintainability Analysis Task.

7.1.5 Testability Design/Analysis - Analyses, evaluation and establishment of testability design concepts, procedures and plans - Results of such a task should be integrated into (or done under the auspices of) the Maintainability Analysis Task and the Maintainability Design Criteria Task.

7.1.6 Testability Demonstration - To determine compliance with specified testability requirements - Testability demonstration should be treated as a portion of the Maintainability Demonstration Task. (See MIL-STD-47ΣA, Notice 2 (Maintainability Verification/Demonstration/Evaluation)

APPENDIX A

A1 Fraction of Faults Detected (FFD) - For the purposes of this document make the following definitions:

Let

F_A = # actual failures (faults) which (will) occur over operating time, T.

F_D = # of actual failures correctly identified through direct observation and other specified means by an operator and/or other specified personnel under a given set(s) of conditions.

$$FFD = \frac{F_D}{F_A}$$

A2 Fraction of Faults Isolated (FFI) - This parameter is usually associated with a maximum ambiguity level (See paragraphs 5.1 and 5.3.1.1). As a consequence, its definition is usually stated in terms of the Fraction of Faults Isolated to a Maximum Ambiguity Level of X Units (Subunits). For the purposes of this document make the following definitions:

Let

F_A = # of actual failures (faults) which (will) occur over operating time T.

F_I = # of actual failures (faults) which (will) occur over operating time T, that can be correctly isolated to X units or fewer at a given maintenance echelon through use of specified diagnostic scheme(s)/test system(s)/procedure(s) (or a defined set of such), by a maintenance technician or other specified personnel.

$$FFI = \frac{F_I}{F_A}$$

A3 False Alarm Rate Ratio - For the purposes of this document make the following definitions:

λ_S = single thread failure rate for system/equipment.

$$\lambda_S = \sum_{i=1}^{i=N} \lambda_i \text{ where;}$$

λ_i = the failure rate of the ith unit of the system/equipment

N= total # of units in the system (assumes all system/equipment units are connected in series)

λ_F = system/equipment rate of occurrence of false alarms where;

$\lambda_F T$ = expected # of system/equipment false alarms in operational time T.

False Alarm Ratio = $\dfrac{\lambda_F}{\lambda_S}$

A4 Fraction of Erroneous Fault Isolation Results (FEFI) - For the purpose of this document make the following definition:

F_A = # of actual failures (faults) which (will) occur over operating time T.

F_E = # of actual failures (faults) which (will) occur over time T, that are isolated to a nonfailed unit or group of units.

FEFI = $\dfrac{F_E}{F_A}$

APPENDIX B

General mix of detection means to be considered for an end item of equipment based on mission criticality of that end item function.

For simplicity let us define three classes of fault detection criticality.

Class I - Mission or Safety Critical - Degraded operation, or operation while in a failed state, even for a short while will jeopardize mission success or personnel and equipment safety.

Class II - Mission or Safety Serious - Degraded operation, or operation while in a failed may adversely impact mission success or personnel and equipment safety.

Class III - Mission or Safety Not Serious - Degraded operation or operation in a failed state will not practically adversely impact mission success or personnel and equipment safety.

(Assumption - Automatic Detection means faster than Semi-Automatic; Semi-Automatic means faster than Manual Means).

The following Table defines the detection means which should be considered and the constraints and interfaces which should be related to each as a function of Fault Detection Criticality.

Classes of Detection Criticality

I	II	III
Detection Maximum possible automatic - cost secondary	Mix of automatic and semi-automatic means - Majority of failures detectable by automatic means - Remainder detectable by semi-automatic means which require operator actions which do not exceed given time maximums derived from mission success and safety considerations. - Detections which require the services of a maintenance technician or periodic inspections by a maintenance technician will be avoided unless it can be demonstrated that no other feasible/practical recourse exists. In that case a schedule for such services/inspections will be developed consistent with mission objectives, mission success criteria and safety needs. - The particular mix of diagnostic means chosen shall be consistent with maintainability requirements and the integrated diagnostics policy.	Mix of automatic, semi-automatic and manual means of fault detection employing the services of either operators or both operators and maintenance technicians working under a prescribed regimen. Consistent with mission needs. - The particular mix of diagnostic means chosen shall be consistent with maintainability requirements and the integrated diagnostics policy.

TABLE B-1